Cyber Defense-in-Depth Is a Smart Investment

A Cyber Security Assumption Buster Workshop Series

Assertion: "Defense-in-Depth is a smart investment because it provides an environment in which we can safely and securely conduct computing functions and achieve mission success."

This assertion reflects a commonly held viewpoint that Defense-in-Depth is a smart investment for achieving perfect safety/security in computing. To analyze this statement we must look at it from two perspectives. First, we need to determine how the cyber security community developed confidence in Defense-in-Depth, and second, we must look at the mechanisms in place to evaluate the cost/benefit of implementing Defense-in-Depth mechanisms.

Initially developed by the military for perimeter protection, Defense-in-Depth was adopted by the National Security Agency (NSA) for main-frame computer system protection. The Defense-in-Depth strategy was designed to provide multiple layers of security mechanisms focusing on people, technology, and operations (including physical security) in order to achieve robust information assurance (IA).[1] Today's highly networked computing environments, however, have significantly changed the cyber security calculus.

Over time, Defense-in-Depth became the *de facto* strategy for providing information assurance to computing systems, and often thought to be able to provide *perfect* security for networking environments.

Defense-in-Depth can provide robust information assurance properties; however, we must consider whether layers of defense may result in *delaying* potential compromise without providing any guarantee that compromise will be completely *prevented*. In today's highly networked world, Defense-in-Depth may best be viewed as a practical way to provide network defense rather than a means to perfect security. It is worth considering whether the Defense-in-Depth strategy tends to contribute more to network *survivability* than is does to network safety/security.

Of particular concern is to determine whether Defense-in-Depth provides a significant barrier to sophisticated, motivated, and determined adversary given those adversaries can structure their attacks to pass through all of the defensive measures and use attack vectors that exploit benign traffic that is authorized to pass through Defense-in-Depth mechanisms.

Cyber Defense-in-Depth Questions:

How do we measure the differential costs accrued by the attacker and the defender when implementing Defense-in-Depth?

How do we shift the differential costs from the attacker to the defender?

How do we measure the value add of additional mechanisms in terms of confidence in the Defense-in-Depth strategy?

Is it better to increase single dimensions rather than developing new dimensions?

How can we develop Defense-in-Depth mechanisms that take into account the Adversarial Threat Model?

How do we defend against a determined adversary by using Defense-in-Depth?

What new avenues for attack are introduced by implementing additional mechanisms to Defense-in-Depth?

Can adversaries create an Offense-in-Depth to counter our Defense-in-Depth?

[1] *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments.*